Journal of Research Proceedings

Under the delegate of "Journal of Research Proceedings," we anchor a bimonthly electronic journal enclosing the diverse realms of the educational research field. JRP is providing a platform for the researchers, academicians, professionals, practitioners, and students to impart and share knowledge in the form of high quality empirical and theoretical research papers, case studies, literature reviews, and book reviews.

JRP Publications
www.i-jrp.com
journalrp.editor@gmail.com
9353189468

Alleviate Insider Statistics Pilferage Blitz in the Cloud

Shruthi S[1], Sandhya B R[2], Ramya H[3]

[1,2,3]Faculty ISE Department, Sri Krishna Institute of Technology, B'lore-560090, India

ABSTRACT

Cloud computing allows to store our personal and business information. you can quickly spin up resources as you need them, deploying hundreds or even thousands of servers in minutes. We propose an approach for data security in the cloud using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. When unauthorized access is suspected and then verified using challenge questions, we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. At the point when unapproved access is suspected and after thatconfirmed utilizing challenge questions, it dispatches a disinformation assault by returning a lot of imitation data to the assailant. This secures against the abuse of the client's genuine information.

KEYWORDS: Cloud Computing, decoy technology, attacker, data security

I. INTRODUCTION

Cloud is used in business sector in recent times. And the cloud becomes a more important part of human life. But protection is big and cloud is a problem. Particularly, insider attack could be much more likely.

In particular, small and medium-sized enterprises, which progressively prefer to outsource data and computation for the cloud. This clearly promotes increased operational performance, but it brings greater risk, perhaps the most extreme of which are data theft attacks, are choosing to start – ups [1].

When the intruder is a malicious user, the data theft attacks are intensified. This is seen on the top challenges to cloud computing from the cyber security alliance while most consumers in the cloud infrastructure industry know this danger well, they can only trust the services provider when it comes to securing their records. This is only compounded by the absence of accountability, let alone power, the security, approval and audit controls offered by the cloud provider. One example of a cloud attack data theft is the twitter event.

A host of studies into online cloud protection based primarily on methods of stopping illicit data access by growing authentication and encryption mechanisms in scale and complexity.

However, these mechanisms could not prevent data compromise. Van Dijk and Juels showed that the frequency adopted as a solution to such problems when used alone, completely holomorphic encryption, does not have appropriate data protection mechanisms [2-3].

We propose a completely different approach to securing the cloud using decoy information technologywhich we call Fog devicesand user behavior profiling,In decoy technology wemislead the attacker with false details and user behavior profiling for user authentication with device based on various user activity parameters. Therefore, here we usethese two technologies to encrypt the cloud data.

II. BACKGROUND STUDY (LITERATURE)

L. Kaufman Et al.(2009)[4] concentrated on the forums of abuses of protection and the related legal and legislative ramifications of cloud computing. Furthermore, a major problem in the specification for the automation of security information was the absence of interoperability between the device level resources. Many that address the vast safety needs of cloud storage separately by blending poisonous best practices and securing the national standards and security center of United States and other parties are emerging. They further improve the security of the details that can conflict with dissemination of events.

The example of cloud protection flaws was presented by Grubaueral.(2012).[5] They outlined the nature of vulnerabilities in the idea that it avoid defending itself from an attack from an asset cant. They said we should even

recognize vulnerabilities in terms of risks and attacks resistance. In particular, control attacks focus situations in which otherwise sufficient protections and inadequate. They represented core cloud technology such as web apps and services that use SaaS and PaaS platforms, virtualization, and said there are many such safety criteria which only cryptographic methods can corrected.

The researchers have also described two additional insider security issues with cloud security, the attacker who uses computer related insecurity to steal information from a cloud-based device. Claycomb R.W. (2012) [6] summarizes a general hierardism of cloud vendor overseers and presents details of actual insider threat-assaults.

Park Y. Et al. (2012) [7] developed an encrypted data protection device decoy strategy. They suggested a program-based decoy device to trick insiders to detect the exfiltration of confidential source code. The Logon contains a Java code that is useful knowledge for the attackers. For the initial device construction and transition the most rigid overloading method is used. Software that is dynamically taken from initial source code but designed to vary from the present is synthesized in error programs. This approach with disappointment confuses the insider, maybe even mysterious, by seeking to dissimulate sensitive details, generating questionable insider knowledge.

Salvador. J StoflioEt al. [8] proposed a fresh tool that Fog computation was known to have. To execute this, they used decoy information technologies. Two aspects, user profiling and Decoy were discusses. They checked how, where and how much information an instant messaging site provides on the user's actions. They started to evaluate their user's actions and verify an irregular data access conduct of the user. The second technology is a decoy where fake information like cookies, honey pots etc., is used to confuse the offender or to demonstrate the details to provide the true appearance.

Madsen and Henrik [9] raised challenges to existing programmatic paradigms and explored the functionality and suitability of fog cloud systems with cloud for projects in real life. Fog computation is primarily because of the need, but instead because of centralized need, for the geographical allocation of resource. A multi layered protection equipment is applied in fog quantum computers.

The multiple hosting vulnerabilities and strategies handled by SabhiF.(2011). [10] He identified the upsides and downsides of the security that have been violated. The paper addresses concerns relating to the trustworthy third party's security and affordability of cloud benefits [11-18]. Distributed access denial attacks are the most recent attacks that he addresses today. The solution to these same assaults was the redundancy of the cloud system, which could deliver functionality more efficiently and deliver early instantly, in order to avoid the site's shutdown. He said that security is the most common hybrid cloud since most user data are saved remotely and the website has to be completely built-in order to fix security issues and malicious intrusions [19-22].

I. METHODOLOGY

The proposed mechanism is to protect information using creativity in the area of aggressive disruption [23]. We screen access to information in the cloud, an identify trends of unusual access to information. At the point where unapproved access is assumed and subsequently verified using challenge queries, a deception assault is dispatched by returning a ton of bait data to attacker [24-29]. This system prescribes a pseudo framework for ensuring information in cloud utilizing summoning fraud elevation. The authorized system shows information entree in cloud and perceive sporadic information arouse plots. Also, when the illegal arouse is grasped and from there on confirmed to raise challenge questions, we hustle a trickiness beset by clearly reestablishing pantomime records to the mugger. Everything just preserves against all the diversion of clarification about its applicant [30-33].

II. IMPLEMENTATION

The decoy files are downloaded by the legitimate user and placed in highly-conspicuous locations that are not likely to cause any interference with the normal user activities on the system [34]. A masquerader, who is not familiar with the file system and its contents, is likely to access these decoy files, if he or she is in search for sensitive information, such as the bait information embedded in these decoy files [35-39]. Therefore, monitoring access to the decoy files should signal masquerade activity on the system. Here pernicious insider means the absence of straight forwardness in cloud suppliers processes and techniques that vindictive leaders may pursue at the noxious assay. It means that a provider cannot know how access is approved for employees and how this admission is observed, or how records and compliances are reviewed in addition. Mist design providers or websites of consumers. The closed details of cloud customers can be reached through the insider. A dangerous one will acquire passwords, encryption keys and documents without much of a run [40-46].

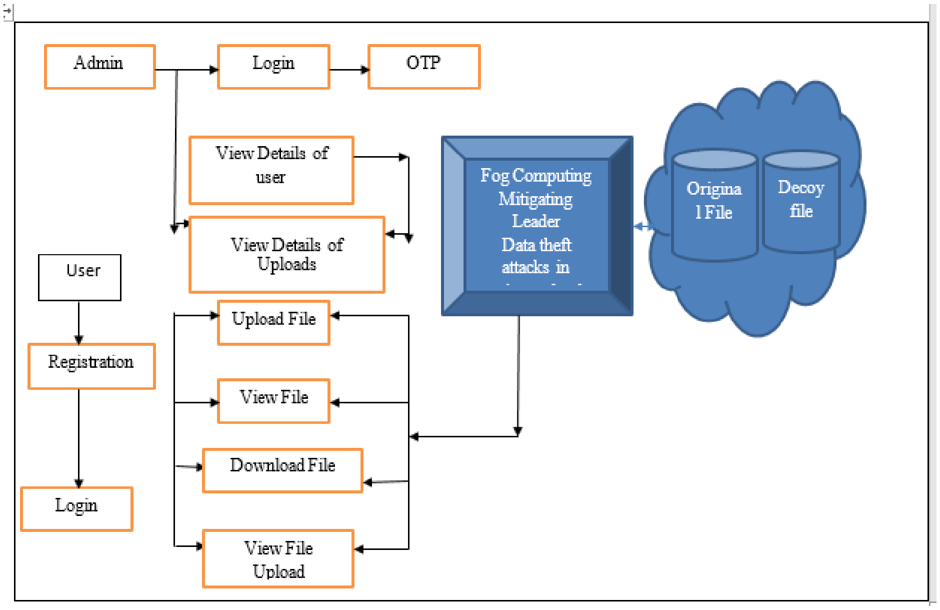

Figure 1: Architecture of System Model

III. CONCLUSION

In this paper we introduced a novel paradigm of security that alludes to as an invention of imitation. In a few crucial respects, baits refer of an aggressive take off of established security arrangements. By throwing faulty yet conceivable content and information in the direction of possible enemies, imitations are an efficient last resort to attacks which customary safety components are not adequately prevented. False compounds are proactively sprouted or nourished as soon as the malicious activity is observed, by a mechanism to defend against future attacks. Especially because of the classification infringement, the following nuisance content should be used after it has existed.

REFERENCES

[1] Seyhan, K., Nguyen, T.N., Akleylek, S., Cengiz, K. and Islam, S.H., 2021. Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security. Journal of Information Security and Applications, 58, p.102788.

[2] Fathima, N., Ahammed, A., Banu, R., Parameshachari, B.D. and Naik, N.M., 2017, December. Optimized neighbor discovery in Internet of Things (IoT). In 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 1-5). IEEE.

[3] Naeem, M.A., Nguyen, T.N., Ali, R., Cengiz, K., Meng, Y. and Khurshaid, T., 2021. Hybrid Cache Management in IoT-based Named Data Networking. IEEE Internet of Things Journal.

[4] Kaufman, L. M. “Data security in the world of cloud computing” in proceedings of IEEE, Security & Privacy, 2009, 7 (4), 61-64.

[5] Grobauer, B., Walloschek, T., & Stocker, E. “Understanding cloud computing vulnerabilities” in proceedings of IEEE, Security & Privacy, 2011, pp. 50-57

[6]Claycomb, William R., and Alex Nicoll. "Insider threats to cloud computing: Directions for new research challenges." In proceedings of Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual, pp. 387-394. IEEE, 2012.

[7] Park, Y., &Stolfo, S. J. “Software decoys for insider threat”, In Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, 2012, May, (pp. 93-94)

[8] Stolfo, Salvatore J., Malek Ben Salem, and Angelos D. Keromytis. "Fog computing: Mitigating insider data theft attacks in the cloud." Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012.

[9] Madsenand Henrik, et al. "Reliability in the utility computing era: Towards reliable Fog computing." Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on. IEEE, 2013.

[10] Sabahi, F. “Cloud computing security threats and responses”, In proceedings of Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on (2011, May), (pp. 245-249).’

[11] Chakraborty, C., Roy, S., Sharma, S., Tran, T., Adhimoorthy, P., Rajagopalan, K. and Jebaranjitham, N., 2021. Impact of Biomedical Waste Management System on Infection Control in the Midst of COVID-19 Pandemic. The Impact of the COVID-19 Pandemic on Green Societiesenvironmental Sustainability, pp.235-262.

[12] Rachana, C.R., Banu, R., Ahammed, G.A. and Parameshachari, B.D., 2017, August. Cloud Computing–A Unified Approach for Surveillance Issues. In IOP Conference Series: Materials Science and Engineering (Vol. 225, No. 1, p. 012073). IOP Publishing.

[13] Chakraborty, C., Roy, S., Sharma, S., Tran, T., Dwivedi, P. and Singha, M., 2021. IoT Based Wearable Healthcare System: Post COVID-19. The Impact of the COVID-19 Pandemic on Green Societiesenvironmental Sustainability, pp.305-321.

[14]DevkarSwapnil, GokhaneAvinash, KaudareJaymala ,KambaleShubham, AbhonkarPrashant,”Survey On Fog computing :Mitigating InsiderData Theft Attack”, in Proceedings of the International Research Journal of Engineering and Technology (IRJET),Volume: 03 Issue, October 2016,p-ISSN: 2395-0072

[15] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," in Proceedings of the First International Workshop on Dependability of Clouds, Data Centers and Virtual Computing Environments, Hong Kong, ser. DCDV '11, June 2011.

[16] Boregowda, S.B., Babu Prasad, N.V., Puttamadappa, C. and Mruthyunjaya, H.S., 2015. Energy Balanced Fixed Clustering protocol for Wireless Sensor Networks. International Journal of Computer Science and Network Security, 11(8), pp.166-172.

[17] Sreevathsa, C.V., Daina, K.K., Hemalatha, K.L. and Manjula, K., 2016, July. Increasing the performance of the firewall by providing customized policies. In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (pp. 561-564). IEEE.

[18] Arun, M., Baraneetharan, E., Kanchana, A. and Prabu, S., 2020. Detection and monitoring of the asymptotic COVID-19 patients using IoT devices and sensors. International Journal of Pervasive Computing and Communications.

[19] M. Van Dijk and A. Juels, "On the impossibility of cryptography alone for privacy-preserving cloud computing," in Proceedings of the 5th USENIX conference on Hot topics in security, ser. HotSec'10. Berkeley, CA, USA: USENIX Association, 2010, pp. 1-8.

[20] M. Ben-Salem and S. J. Stolfo, "Modeling user search-behavior for masquerade detection," in Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, September 2011, pp. 1-20.

[21] K. Yu, L. Tan, L. Lin, X. Cheng, Z. Yi and T. Sato, "Deep-Learning-Empowered Breast Cancer Auxiliary Diagnosis for 5GB Remote E-Health," IEEE Wireless Communications, vol. 28, no. 3, pp. 54-61, June 2021, doi: 10.1109/MWC.001.2000374.

[22] K. Yu, L. Tan, S. Mumtaz, S. Al-Rubaye, A. Al-Dulaimi, A. K. Bashir, F. A. Khan, “Securing Critical Infrastructures: Deep Learning-based Threat Detection in the IIoT”, IEEE Communications Magazine, 2021.

[23] K. Yu, Z. Guo, Y. Shen, W. Wang, J. C. Lin, T. Sato, “Secure Artificial Intelligence of Things for Implicit Group Recommendations”, IEEE Internet of Things Journal, 2021, doi: 10.1109/JIOT.2021.3079574.

[24] Parameshachari, B. D., H. T. Panduranga, and S. K. Naveenkumar. "Partial encryption of medical images by dual DNA addition using DNA encoding." In *2017 international conference on recent innovations in signal processing and embedded systems (RISE)*, pp. 310-314. IEEE, 2017.

[25] Shahriar, Md Rakib, SM Nahian Al Sunny, Xiaoqing Liu, Ming C. Leu, Liwen Hu, and Ngoc-Tu Nguyen. "MTComm based virtualization and integration of physical machine operations with digital-twins in cyber-physical manufacturing cloud." In *2018 5th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2018 4th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pp. 46-51. IEEE, 2018.

[26] Parameshachari, B. D., H. T. Panduranga, and Silvia liberata Ullo. "Analysis and computation of encryption technique to enhance security of medical images." In *IOP Conference Series: Materials Science and Engineering*, vol. 925, no. 1, p. 012028. IOP Publishing, 2020.

[27] Nguyen, Tu N., Bing-Hong Liu, Nam P. Nguyen, and Jung-Te Chou. "Cyber security of smart grid: attacks and defenses." In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2020.

[28] Le, Ngoc Tuyen, Jing-Wein Wang, Duc Huy Le, Chih-Chiang Wang, and Tu N. Nguyen. "Fingerprint enhancement based on tensor of wavelet subbands for classification." *IEEE Access* 8 (2020): 6602-6615.

[29] Rajendran, Ganesh B., Uma M. Kumarasamy, Chiara Zarro, Parameshachari B. Divakarachari, and Silvia L. Ullo. "Land-use and land-cover classification using a human group-based particle swarm optimization algorithm with an LSTM Classifier on hybrid pre-processing remote-sensing images." *Remote Sensing* 12, no. 24 (2020): 4135.

[30] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv and S. Mumtaz, "Attribute-Based Encryption with Parallel Outsourced Decryption for Edge Intelligent IoV," IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13784-13795, Nov. 2020, doi: 10.1109/TVT.2020.3027568.

[31] S. Chen, L. Zhang, Y. Tang, C. Shen, R. Kumar, K. Yu, U. Tariq, and A. K. Bashir, “Indoor Temperature Monitoring Using Wireless Sensor Networks: A SMAC Application in Smart Cities”, Sustainable Cities and Society, vol. 61, p. 102333, July 2020.

[32] W. Zeng, Z. Guo, Y. Shen, A. K. Bashir, K. Yu, Y. D. Al-Otaibi, and X. Gao, “Data-Driven Management for Fuzzy Sewage Treatment Processes Using Hybrid Neural Computing”, Neural Computing and Applications, https://doi.org/10.1007/s00521-020-05655-3.

[33] Subramani, Prabu, K. Srinivas, R. Sujatha, and B. D. Parameshachari. "Prediction of muscular paralysis disease based on hybrid feature extraction with machine learning technique for COVID-19 and post-COVID-19 patients." *Personal and Ubiquitous Computing* (2021): 1-14.

[34] Hemalatha, K. L., S. M. Ashitha, and S. R. Meghana. "Design and implementation of modified FCM in the detection of brain tumor." *Int. J. Adv. Sci. Res. Eng* 3, no. 4 (2017): 2850-2858.

[35] Puttamadappa, C., and B. D. Parameshachari. "Demand side management of small scale loads in a smart grid using glow-worm swarm optimization technique." *Microprocessors and Microsystems* 71 (2019): 102886.

[36] Hu, Liwen, Ngoc-Tu Nguyen, Wenjin Tao, Ming C. Leu, Xiaoqing Frank Liu, Md Rakib Shahriar, and SM Nahian Al Sunny. "Modeling of cloud-based digital twins for smart manufacturing with MT connect." *Procedia manufacturing* 26 (2018): 1193-1203.

[37] Subramani, Prabu, Ganesh Babu Rajendran, Jewel Sengupta, Rocío Pérez de Prado, and Parameshachari Bidare Divakarachari. "A block bi-diagonalization-based pre-coding for indoor multiple-input-multiple-output-visible light communication system." *Energies* 13, no. 13 (2020): 3466.

[38] Liu, Bing-Hong, Ngoc-Tu Nguyen, Van-Trung Pham, and Yue-Xian Lin. "Novel methods for energy charging and data collection in wireless rechargeable sensor networks." *International Journal of Communication Systems* 30, no. 5 (2017): e3050.

[39] Parameshachari, B. D., Rashmi P. Kiran, P. Rashmi, M. C. Supriya, Rajashekarappa, and H. T. Panduranga. "Controlled partial image encryption based on LSIC and chaotic map." In *ICCSP*, pp. 60-63. 2019.

[40] Nguyen, Ngoc-Tu, and Bing-Hong Liu. "The mobile sensor deployment problem and the target coverage problem in mobile wireless sensor networks are NP-hard." *IEEE Systems Journal* 13, no. 2 (2018): 1312-1315.

[41] Hemalatha, K. L., SUNILKUMAR MANVI, and HN SURESH. "ADAPTIVE WEIGHTED-COVARIANCE REGULARIZED KERNEL FUZZY C MEANS ALGORITHM FOR MEDICAL IMAGE SEGMENTATION." *Journal of Theoretical & Applied Information Technology* 95, no. 14 (2017).

[42] Bhuvaneswary, N., S. Prabu, K. Tamilselvan, and K. G. Parthiban. "Efficient Implementation of Multiply Accumulate Operation Unit Using an Interlaced Partition Multiplier." *Journal of Computational and Theoretical Nanoscience* 18, no. 4 (2021): 1321-1326.

[43] Subramani, Prabu, Fadi Al-Turjman, Rajagopal Kumar, Anusha Kannan, and Anand Loganthan. "Improving medical communication process using recurrent networks and wearable antenna s11 variation with harmonic suppressions." *Personal and Ubiquitous Computing* (2021): 1-13.

[44] Z. Guo, Y. Shen, A. K. Bashir, M. Imran, N. Kumar, D. Zhang and K. Yu, "Robust Spammer Detection Using Collaborative Neural Network in Internet of Thing Applications", IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9549-9558, 15 June15, 2021, doi: 10.1109/JIOT.2020.3003802.

[45] L. Tan, H. Xiao, K. Yu, M. Aloqaily, Y. Jararweh, "A Blockchain-empowered Crowdsourcing System for 5G-enabled Smart Cities", Computer Standards & Interfaces, https://doi.org/10.1016/j.csi.2021.103517

[46] C. Feng et al., "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," IEEE Network, vol. 35, no. 1, pp. 130-137, January/February 2021, doi: 10.1109/MNET.011.2000223.